ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20275—2006

信息安全技术
入侵检测系统技术要求和测试评价方法

**Information security technology—
Techniques requirements and testing and evaluation approaches for intrusion detection system**

2006-05-31 发布　　2006-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 20275—2006

中华人民共和国
国家标准
信息安全技术
入侵检测系统技术要求和测试评价方法
GB/T 20275—2006
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 3.25　字数 88 千字
2006年10月第一版　2006年10月第一次印刷
*
书号:155066·1-28090　定价 21.00 元

GB/T 20275-2006

参 考 文 献

[1] GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求(idt ISO/IEC 15408-2:1999)

[2] GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求(idt ISO/IEC 15408-3:1999)

目 次

7.5.3.6.3 **功能测试**

a) 测试评价方法：

1) 评价开发者提供的测试文档，是否包含测试计划、测试规程、预期的测试结果和实际测试结果；

2) 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

3) 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

4) 评价期望的测试结果是否表明测试成功后的预期输出；

5) 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b) 测试评价结果：测试记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的5方面。开发者提供的内容应完整。

7.5.3.6.4 **独立性测试**

a) 测试评价方法：评价者应审查开发者是否提供了用于测试的产品，且提供的产品是否适合测试。

b) 测试评价结果：测试记录以及最后结果（符合/不符合），开发者应提供能适合第三方测试的产品。

7.5.3.7 **脆弱性评定**

7.5.3.7.1 **指南检查**

a) 测试评价方法：

评价者应审查开发者提供的文档，是否满足了以下要求：

1) 评价文档，是否确定了对产品的所有可能的操作方式（包括失败和操作失误后的操作），是否确定了它们的后果，以及是否确定了对于保持安全操作的意义；

2) 评价文档，是否列出了所有目标环境的假设以及所有外部安全措施（包括外部程序的、物理的或人员的控制）的要求；

3) 评价文档是否完整、清晰、一致、合理；

4) **评价开发者提供的分析文档，是否阐明文档是完整的。**

b) 测试评价结果：测试记录以及最后结果（符合/不符合）符合测试评价方法要求。开发者提供的评价文档应完整，**并且通过分析文档等方式阐明文档是完整的。**

7.5.3.7.2 **脆弱性分析**

a) 测试评价方法：

1) 评价开发者提供的脆弱性分析文档，是否从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行了分析；

2) 对被确定的脆弱性，评价开发者是否明确记录了采取的措施；

3) 对每一条脆弱性，评价是否有证据显示在使用产品的环境中该脆弱性不能被利用。

b) 测试评价结果：测试记录以及最后结果（符合/不符合）符合测试评价方法要求。开发者提供的脆弱性分析文档应完整。